

Agence Nationale
des Systèmes d'information
de l'état

Djibouti le, 09-06-2024

BULLETIN ALERTES

Object	Multiples Vulnérabilités dans le noyau Linux de Red Hat
Référence	1159
Date de Publication	2024-06-07
Sévérité	Elevé

IMPACT :

- Atteinte à l'intégrité des données
- Atteinte à la confidentialité des données
- Déni de service à distance
- Contournement de la politique de sécurité
- Élévation de privilèges
- Non spécifié par l'éditeur

SYSTÈME AFFECTÉ :

- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 8 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 9 aarch64
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat CodeReady Linux Builder for x86_64 8 x86_64

- Red Hat CodeReady Linux Builder for x86_64 9 x86_64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat Enterprise Linux for ARM 64 9 aarch64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for Real Time - Telecommunications Update Service 8.4 x86_64
- Red Hat Enterprise Linux for Real Time 8 x86_64
- Red Hat Enterprise Linux for Real Time 9 x86_64
- Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.4 x86_64
- Red Hat Enterprise Linux for Real Time for NFV 8 x86_64
- Red Hat Enterprise Linux for Real Time for NFV 9 x86_64
- Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.4 x86_64
- Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64
- Red Hat Enterprise Linux for x86_64 8 x86_64
- Red Hat Enterprise Linux for x86_64 9 x86_64
- Red Hat Enterprise Linux Server - AUS 8.2 x86_64
- Red Hat Enterprise Linux Server - AUS 8.4 x86_64
- Red Hat Enterprise Linux Server - AUS 9.4 x86_64
- Red Hat Enterprise Linux Server - TUS 8.4 x86_64
- Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.4 aarch64
- Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.4 s390x
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le

DÉSCRIPTION :

Des nombreuses vulnérabilités ont été découvertes dans le noyau Linux de Red Hat susmentionné. Certaines d'entre elles permettent à un attaquant de provoquer une élévation de privilèges, un déni de service à distance et une atteinte à la confidentialité des données.

SOLUTION :

Mettre à jour vos systèmes Red Hat. (se réfère à la documentation)

DOCUMENTATION :

- Bulletin de sécurité Red Hat RHSA-2024:3528 du 31 mai 2024

<https://access.redhat.com/errata/RHSA-2024:3528>

- Bulletin de sécurité Red Hat RHSA-2024:3529 du 31 mai 2024

<https://access.redhat.com/errata/RHSA-2024:3529>

- Bulletin de sécurité Red Hat RHSA-2024:3530 du 31 mai 2024

<https://access.redhat.com/errata/RHSA-2024:3530>

- Bulletin de sécurité Red Hat RHSA-2024:3618 du 05 juin 2024

<https://access.redhat.com/errata/RHSA-2024:3618>

- Bulletin de sécurité Red Hat RHSA-2024:3619 du 05 juin 2024

<https://access.redhat.com/errata/RHSA-2024:3619>

- Bulletin de sécurité Red Hat RHSA-2024:3627 du 05 juin 2024

<https://access.redhat.com/errata/RHSA-2024:3627>

- CVE-2019-25162

<https://www.cve.org/CVERecord?id=CVE-2019-25162>

- CVE-2020-36777

<https://www.cve.org/CVERecord?id=CVE-2020-36777>

- CVE-2021-46934

<https://www.cve.org/CVERecord?id=CVE-2021-46934>

- CVE-2021-47013

<https://www.cve.org/CVERecord?id=CVE-2021-47013>

- CVE-2021-47055

<https://www.cve.org/CVERecord?id=CVE-2021-47055>

- CVE-2021-47118

<https://www.cve.org/CVERecord?id=CVE-2021-47118>

- CVE-2021-47153

<https://www.cve.org/CVERecord?id=CVE-2021-47153>

- CVE-2021-47171

<https://www.cve.org/CVERecord?id=CVE-2021-47171>

- CVE-2021-47185

<https://www.cve.org/CVERecord?id=CVE-2021-47185>

- CVE-2022-48627

<https://www.cve.org/CVERecord?id=CVE-2022-48627>

- CVE-2022-48669

<https://www.cve.org/CVERecord?id=CVE-2022-48669>

- CVE-2023-2166

<https://www.cve.org/CVERecord?id=CVE-2023-2166>

- CVE-2023-2176

<https://www.cve.org/CVERecord?id=CVE-2023-2176>

- CVE-2023-52439

<https://www.cve.org/CVERecord?id=CVE-2023-52439>

- CVE-2023-52445

<https://www.cve.org/CVERecord?id=CVE-2023-52445>

- CVE-2023-52477

<https://www.cve.org/CVERecord?id=CVE-2023-52477>

- CVE-2023-52513

<https://www.cve.org/CVERecord?id=CVE-2023-52513>

- CVE-2023-52520

<https://www.cve.org/CVERecord?id=CVE-2023-52520>

- CVE-2023-52528

<https://www.cve.org/CVERecord?id=CVE-2023-52528>

- CVE-2023-52565

<https://www.cve.org/CVERecord?id=CVE-2023-52565>

- CVE-2023-52578

<https://www.cve.org/CVERecord?id=CVE-2023-52578>

- CVE-2023-52594

<https://www.cve.org/CVERecord?id=CVE-2023-52594>

- CVE-2023-52595

<https://www.cve.org/CVERecord?id=CVE-2023-52595>

- CVE-2023-52598

<https://www.cve.org/CVERecord?id=CVE-2023-52598>

- CVE-2023-52606

<https://www.cve.org/CVERecord?id=CVE-2023-52606>

- CVE-2023-52607

<https://www.cve.org/CVERecord?id=CVE-2023-52607>

- CVE-2023-52610

<https://www.cve.org/CVERecord?id=CVE-2023-52610>

- CVE-2023-6240

<https://www.cve.org/CVERecord?id=CVE-2023-6240>

- CVE-2024-0340

<https://www.cve.org/CVERecord?id=CVE-2024-0340>

- CVE-2024-1086

<https://www.cve.org/CVERecord?id=CVE-2024-1086>

- CVE-2024-23307

<https://www.cve.org/CVERecord?id=CVE-2024-23307>

- CVE-2024-25744

<https://www.cve.org/CVERecord?id=CVE-2024-25744>

- CVE-2024-26593

<https://www.cve.org/CVERecord?id=CVE-2024-26593>

- CVE-2024-26603

<https://www.cve.org/CVERecord?id=CVE-2024-26603>

- CVE-2024-26610

<https://www.cve.org/CVERecord?id=CVE-2024-26610>

- CVE-2024-26615

<https://www.cve.org/CVERecord?id=CVE-2024-26615>

- CVE-2024-26642

<https://www.cve.org/CVERecord?id=CVE-2024-26642>

- CVE-2024-26643

<https://www.cve.org/CVERecord?id=CVE-2024-26643>

- CVE-2024-26659

<https://www.cve.org/CVERecord?id=CVE-2024-26659>

- CVE-2024-26664

<https://www.cve.org/CVERecord?id=CVE-2024-26664>

- CVE-2024-26693

<https://www.cve.org/CVERecord?id=CVE-2024-26693>

- CVE-2024-26694

<https://www.cve.org/CVERecord?id=CVE-2024-26694>

- CVE-2024-26735

<https://www.cve.org/CVERecord?id=CVE-2024-26735>

- CVE-2024-26743

<https://www.cve.org/CVERecord?id=CVE-2024-26743>

- CVE-2024-26744

<https://www.cve.org/CVERecord?id=CVE-2024-26744>

- CVE-2024-26779

<https://www.cve.org/CVERecord?id=CVE-2024-26779>

- CVE-2024-26872

<https://www.cve.org/CVERecord?id=CVE-2024-26872>

- CVE-2024-26892

<https://www.cve.org/CVERecord?id=CVE-2024-26892>

- CVE-2024-26897

<https://www.cve.org/CVERecord?id=CVE-2024-26897>

- CVE-2024-26901

<https://www.cve.org/CVERecord?id=CVE-2024-26901>

- CVE-2024-26919

<https://www.cve.org/CVERecord?id=CVE-2024-26919>

- CVE-2024-26933

<https://www.cve.org/CVERecord?id=CVE-2024-26933>

- CVE-2024-26934

<https://www.cve.org/CVERecord?id=CVE-2024-26934>

- CVE-2024-26964

<https://www.cve.org/CVERecord?id=CVE-2024-26964>

- CVE-2024-26973

<https://www.cve.org/CVERecord?id=CVE-2024-26973>

- CVE-2024-26993

<https://www.cve.org/CVERecord?id=CVE-2024-26993>

- CVE-2024-27014

<https://www.cve.org/CVERecord?id=CVE-2024-27014>

- CVE-2024-27048

<https://www.cve.org/CVERecord?id=CVE-2024-27048>

- CVE-2024-27052

<https://www.cve.org/CVERecord?id=CVE-2024-27052>

- CVE-2024-27056

<https://www.cve.org/CVERecord?id=CVE-2024-27056>

- CVE-2024-27059

<https://www.cve.org/CVERecord?id=CVE-2024-27059>